REMARKS/ARGUMENTS

Claims 1 – 27 are pending in the application. Claims 1, 10, 22, and 27 have been amended. Support for the amendments is found in the specification, drawings, and claims as originally filed. Applicants respectfully submit, therefore, that the amendments do not add new matter.

Claims Rejections – 35 USC §103

In the June 14, 2006 Office Action, Claims 1-8, 10-14, 16-18, 20 , 21, 26 and 27 were rejected under 35 U.S.C. § 103 as allegedly being unpatentable over U.S. Patent No. 6,003,135 to Bialick et al. ("Bialick") in view of U.S. Patent No. 6,671,809 to Perona et al. ("Perona"). Claims 9 and 22-25 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bialick in view of U.S. Patent No. 6,374,315 to Okada et al. ("Okada") and Perona. Claims 15 and 19 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bialick in view of Perona and U.S. Patent No. 6,134,593 to Alexander et al. ("Alexander").

Finally, Claim 9 was rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bialick in view of Perona and Okada.

Applicant respectfully submits that the invention, as claimed, for example, in amended claim 1, is not anticipated by Bialick. Claim 1 includes the following limitations.

> A method comprising: in a portable data device, checking a wireless network card for a stored platform discrimination indication, the platform discrimination indication dependent upon a wireless data transfer capacity of the portable data device; and depending on a value of the platform discrimination indication, inhibiting or allowing data transfer, across a wireless network, using the wireless network card.

(Amended claim 1) (Emphasis added)

Applicants respectfully submit that Bialick does not disclose the limitation of a data transfer across a wireless network that is dependent upon a platform discrimination indication of a wireless network card, where the platform discrimination indication is dependent upon a wireless data transfer capacity of a portable data device.

As cited by the Examiner, Bialick discloses the following.

> In the system 200, if it is desired to provide secured data from the host computing device 201 to the portable device 202, the host computing device 201 first causes data to be transferred to the security device 203, where appropriate cryptographic operations are performed on the data. The secured data is then transferred back to the host computing device 201, which, in turn, transfers the secured data to the portable device 202. Similarly, the host computing device 201 can receive secured data from the portable device 202 by, upon receipt of secured data, transferring the secured data to the security device 203, which performs appropriate cryptographic operations on the data to convert the data into a form that enables the data to be accessed and/or modified by a person who is authorized to do so, then transfers the unsecured data back to the host computing device 201.

(Bialick, col. 2, lines 32 – 47)

> Once connection between the modular device and the host computing device is made, the host computing device detects the presence of the modular device, as shown by step 502. Such detection of the presence of a peripheral device is typically enabled as a standard aspect of the operating system software of the host computing device.
>
> Typically, once the presence of a new peripheral device is detected by the operating system software of the host computing device, the operating system software (or companion software program) also identifies the type of the peripheral device. This can be accomplished, for example, by a standard software device driver (hereinafter, "host driver") for devices of the type that use the host computing device interface that is being used by the modular device 602. In FIG. 6, the host driver is shown stored in the memory section 606a of the memory device 606 of the host computing device 601. (The Card Services or Socket Services programs that often are bundled with the Windows95.TM. operating system software for use in performing various "housekeeping" functions associated with a PCMCIA interface are examples of such drivers.) However, in the method 500, before the operating system software can perform such identification, the modular device according to the invention suspends operation of this aspect of the operating system software, so that the modular device can establish its identity, as shown by step 503, and explained further below. As will be apparent from that explanation, performance of the step 503 advantageously enables the modular device to assume the identity of the target module that is part of the modular device at that time. Since, as described elsewhere herein, a

variety of types of target modules can be used as part of a modular device according to the invention, the modular device can take a variety of identities.

(Bialick, col. 9, line 45 – col. 10, line 10)

As indicated above, a modular device according to the invention can be implemented so that, when a target module is present as part of the modular device, the host driver cannot detect the presence of the security functionality of the modular device. In such case, the modular device driver enables the detection of the security functionality, as shown by step 702 of the method 700. This can be accomplished by including instructions as part of the modular device driver that, when the modular device driver first begins executing, cause the modular device driver to access a predefined location of a memory device of the modular device (preferably, and as described above, a memory device of a security module of the modular device) for data that identifies whether the modular device is a device having security functionality that is compatible with the modular device driver. (In FIG. 6, this is shown as the memory section 612b.) If the modular device is such a device, then the modular device driver can enable the user to make use of the security functionality of the modular device. Further, the modular device driver can be implemented, as shown in FIG. 7, so that, if the proper security functionality is not detected, execution of the modular device driver terminates, preventing use of the modular device. Alternatively, the modular device driver can be implemented so that, if the proper security functionality is not detected, the functionality of a target module of the modular device can be used without the security functionality of the modular device.

A modular device according to the invention that includes a security module and a target module can, in general, be operated in one of three modes: 1) a mode in which only the functionality of the security module is used, 2) a mode in which the functionality of both the security and the target modules is used, and 3) a mode in which only the functionality of the target module is used. The user can be enabled to, via the modular device driver, select any one of the three modes of operation. However, in some applications, it may be desirable to inhibit operation in one or two of the modes. In particular, it may be desirable to prevent operation of the modular device in the last of the above-listed modes, i.e., a mode in which the security module is not used, if it is desired to ensure that use of the target module can only occur with the application of one or more security operations. This could be accomplished by implementing the modular device driver so that the option to operate in that mode is not presented to the user, or the modular device could be configured during manufacture to prohibit operation in that mode. For example, if the target module is a communications module or a memory module, it may be desirable to ensure that unencrypted data cannot be transferred via the communications module or stored on the memory module, whether done inadvertently or on purpose.

(Bialick, col. 13, lines 11 - 61)

Bialick et al. discloses a modular device that communicates with a host computing device and enables security operations to be performed by the modular device on: (i) data stored within the host computing device, (ii) data provided from the host computing device to the modular device, or data retrieved by the host computing device from the modular device. The modular device includes a security module that is adapted to enable performance of the security operations on the data and a target module that is adapted to enable a defined interaction with the host computing device. The target module can be embodied by any of a variety of modules having different types of functionality (e.g. data storage, data communication, data input and output, user identification).

Bialick does not disclose or suggest the limitation of data transfer across a wireless network dependent upon a data transfer capacity of a wireless device. Moreover, Bialick does not disclose or suggest the limitation of checking the wireless network card for a stored platform discrimination indication on which would depend the transfer of data across a wireless network where the platform discrimination indication dependent upon a wireless data transfer capacity of a portable data device.

For these reasons, applicants respectfully submit that the present claims are neither anticipated nor rendered obvious by Bialick. Applicants further respectfully submit that none of the additional cited references, alone or in combination, remedy the deficiencies of Bialick in this regard.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 408-282-1809.

Respectfully submitted,

Dated: 9/14/06

Thomas Van Zandt
Reg. No. 43,219

THELEN REID & PRIEST LLP
P.O. Box 640640
San Jose, CA 95164-0640
(408) 282-1809 Telephone
(408) 287-8040 Facsimile